TEXAS
Department of Aging
and Disability Services

COMMISSIONER
James R. Hine

September 17, 2004

To: Medicaid-Certified Nursing Facility Providers

Subject: Provider Letter 04-26
Reinstating Access to the Nursing Home Form Suspense and Error Report
Effective August 27, 2004 (Replaces Provider Letter 04-17)

Due to system upgrades, electronic access to the Nursing Home Form Suspense and Error report was placed on hold. This letter is to inform nursing facility providers that, effective August 27, 2004, you have electronic access to the suspense and error report. This report contains Transaction Notices, Forms 3618 and 3619, and the Client Assessment and Evaluation, Form 3652, which has suspended or errored in the system and, therefore, cannot be processed for payment. This is the same report that providers receive bi-monthly by mail. It can be accessed electronically every Wednesday, with the effective date of the report data reflected in the “data as of” field. The suspense and error report will be available via a secured Web page at the Texas Department of Aging and Disability Services (DADS) website shown below:

http://txnfsr.dhs.state.tx.us/NFSRWeb/app/home

(NOTE: The above website address differs from the website address in the May 2004 release.)

Instructions for obtaining a User-ID, Password and Access Authorization

The attached Forms 4743 and 4014 must be completed as directed below, signed and faxed to (512) 438-5288 to be assigned a User-ID and password for access. Login procedures are available under the “Help” icon once you access the site.

If you previously submitted Forms 4743 and 4014 requesting access and have not received a User-ID and password, contact the Enterprise Help Desk at (512) 438-4720, press “0” for an operator and refer to the above-shown website address.

FORM 4743 - Unless form field is identified below, please leave blank.

∝	Field - “Type of USER Change”	- Enter **Add New**
∝	Field - “Employee Name”	- Enter **Nursing Facility Name**
∝	Field - “Employee No.”	- Enter **Nursing Facility Contract Number (9-digit)**
∝	Field - “Employee Phone No.”	- Enter **Nursing Facility Fax Number**
∝	Field - “E-mail”	- Enter **Nursing Facility E-mail address**
	Field - “Employee Title/Contractor”	- Enter **Nursing Facility Administrator’s Name**
∝	Item #14 - “Other”	- Enter **Nursing Home Suspense & Error Report**

∝ Field - “Print Name – Supervisor”	- Enter **Nursing Facility Administrator’s Name**
∝ Field - “Signature – Supervisor”	- Enter **Nursing Facility Administrator’s Signature**
∝ Field - “Date”	- Enter **Date signed**
∝ Field - “Phone”	- Enter **Administrator’s Telephone Number**

FORM 4014 - Unless form field is identified below, please leave blank.

∝ Field - “Name”	- Enter **Nursing Facility Administrator’s Name**
∝ Field - “ Social Security No.”	- Enter **Nursing Facility Contract Number (9-digit)**
∝ Field - “Provider Agency Name”	- Enter **Nursing Facility Name**
∝ Field - “Signature”	- Enter **Signature of Administrator**
∝ Field - “Date”	- Enter **Date signed**

The User-ID and password will be faxed to the facility number entered on the Form 4743. Once logged into the website, you will be prompted to change the password; you will be prompted similarly every 90 days thereafter for security purposes.

The ability to access this report electronically will allow the provider a quicker response time to resolve form issues that need to be corrected. If you have any questions regarding the report, please contact the Texas Health and Human Services Commission, Provider Claims Services, at (512) 490-4666.

Sincerely,

[signature on file]

Veronda L. Durden
Assistant Deputy Commissioner
Regulatory Services

VLD:ca

Attachments

Texas Health and Human
Services Commission

Request for Applications and System Access

Form 4743
September 2004

FAX TO: **Management Information Services**
State Office C-732, FAX (512) 438-5288

FROM:

FOR SECURITY SECTION USE ONLY	Identifier	Password	Password	Password	Password

System Designator	City	Region	Mail Code	Type of **USER** Change □ **Add New** □ **Delete** □ **Modify**

Employee Name (last, first, MI) Name as appears in AASS	Effective/Hire/Termination Date	BJN

Employee No.	Social Security No.	Employee Phone No. (inc. area code & extension)

E-Mail	Employee Title / Contractor

IRIS: □ Production □ Development □ Mapper Dept./Mode: ______________________

TEXAS HEALTH AND HUMAN SERVICES COMMISSION:

___ 1. Non-LAN Financial Servs ___Limited Inq ___Full Inq
___ 2. Non-LAN Financial Servs Data Entry
___ 3. FMIS ___Inq ___DE
___ 4. HRMIS ___SO ___REG ___ Inq ___ DE
___ 5. Medical Provider Services Inquiry
___ 6. ___ LAN ___ LSC
___ 7. TAMENU

___ 8. Texas Works ___ Clerk ___ Worker
___ 9. LTCS ___ Clerk ___ Worker
___ 10. BCMAST ___ Inq ___ DE
___ 11. TWC
___ 12. OAG
___ 13. Broadcast ___ Texas Works ___ LTCS
___ 14. Other ______________________

CLIENT SERVER/RMO APPLICATIONS:

___ 1. OUTLOOK
___ 2. DATA BROKER
___ 3. WTPY
___ 4. IRS
___ 5. DIAL-UP
___ 6. ARTS WEB
___ 7. MDS

___ 8. OPI
___ 9. CASE TRACKING APP for OGC
___ 10. CARES
___ 11. ALZHEIMERS
___ 12. TEXAS WORKS REDIRECTS
___ 13. TEXAS WORKS SCHEDULER
___ 14. ASPEN

___15. CMS ___ SASO ___ PROVIDER
___16. CCAD CASELOAD REALIGNMENT
___17. IWS / INCOME & ELIGIBILITY VERIFICATION SYSTEM
___18. PMRS
___19. PMRS PROJECT MANAGER/LIBRARIAN
___20. RMO Applications: ______________________
___21. Other ______________________

CLIENT SERVER DATABASE:

Server : ______________ □ **Add** □ **Delete** □ **Modify**

Database/Schema	Group/Alias/Role	Effective Begin Date	Effective End Date	**DBA Use Only** Action Taken

DBA USE ONLY:

Login: ______________ Completed By: ______________ Date User Notified: ______________

Password: ______________ Completed Date: ______________

UNIX:

□ **User** □ **Administrator** **Required Access Dates**

System: ______________ Request Group: ______________ Start: ______________

Alternate Directory: ______________ Preferred Shell: ______________ End: ______________

______________ ______________ ______________ ______________
Print Name - Supervisor **Signature** - Supervisor Date Phone #

Comments:

______________ ______________
Signature - Regional Automation Director Date

FOR SECURITY SECTION USE ONLY

□ **Approved** □ **Disapproved**

Reg. Comments: ______________________

MIS Comments: ______________________

PAC: ______________________

______________ ______________
Signature - Security Date

RD/RMO: ______________________

Texas Health and Human
Services Commission

Form 4014
September 2004

Computer Security Agreement

Name	Social Security No.	Div./Reg. (1st 3 digits of BJN)	Unit (4th and 5th digits of BJN)	Mail Code
Provider Agency Name		Business Telephone No. (inc. area code and extension) ( ) – Ext.		

The following policies and procedures exist to provide information security, protect privacy, and ensure the confidentiality and integrity of client, employee, and administrative data accessed via automated systems within the Texas Department of Aging and Disability Services (DADS) or from other systems outside DADS. Please read the following agreement carefully and thoroughly before signing.

I understand that in performance of my assigned job duties, or in connection with services I am required or authorized to perform on behalf of DADS, I may receive DADS identification codes (ID) and/or passwords (also known as security codes) to DADS information resources. I understand that any issued IDs and/or passwords are for official state-approved business only. I understand that the IDs and/or passwords are to be used only by me, and that I am not to disclose my passwords to anyone or allow anyone to use my IDs and/or passwords. I understand that I am responsible for any actions performed under my ID. I agree to change my passwords every 90 days or immediately should they become compromised; for example, if someone learns my password or the password becomes known during problem resolution or day-to-day functions.

I understand that I am prohibited from changing any software (including, but not limited to, display screens, operating system instructions, and applications) that reside on any DADS system or automated storage medium unless this change is approved by an authorized person.

I understand that I am prohibited from accessing any automated system, subsystem, or automated storage medium for which I have not previously received proper authorization. I further understand that I am prohibited from altering any data or database other than that which is specifically authorized as required in the performance of my job functions.

I understand that if I have any questions or problems, I am to immediately report the situation to my supervisor, automation support staff, information security staff, or other individual designated as the point of contact with DADS under any contract pursuant to which I perform services on behalf of DADS.

I agree to follow policies and procedures related to information security and data confidentiality in handbooks and manuals issued by DADS automation authorities and any additions, deletions, or revisions thereto.

I agree that, without written approval from DADS, I will not disclose any information obtained from DADS to any outside entity, and no written information will be removed from DADS premises.

I have read Form 4014, Pages 1 and 4, related to information security and data confidentiality. I understand that these and the above stated policies and procedures apply to all security codes or other access rights I receive to conduct state-related business. I understand that failure to follow the policies, procedures, and laws of the State of Texas may result in loss of access to the computer system(s) and/or disciplinary action, which may include dismissal, exercise of remedies for breach of contract, termination of my contract, and/or criminal prosecution.

Signature

Date

Computer Security Agreement

As an authorized user of the Internal Revenue Service (IRS) Match Inquiry System, I understand the information obtained from the system may be used for official state-approved business. I understand my user ID and password is to be used only by me. Under no circumstances will I reveal or allow use of my password by another person.

I understand printed IRS inquiries must be stored in a locked container or room and printed IRS data must be destroyed according to confidential trash procedures established by DADS.

I understand if I fail to follow any of these standards, I may be subject to disciplinary action, exercise of remedies for breach of contract, termination of contract, and/or prosecution. Unauthorized disclosure of IRS data can result in a felony conviction punishable by a fine up to $5,000 and/or up to five years in prison.

I understand and agree to follow the security procedures stated in this agreement.

______________________________	____________
Signature	Date

Program Area Approval for Non-State Staff ______________________________

Data Broker

As an authorized user of the Data Broker system, I understand the information obtained from the system shall be used only for official state-approved business. I understand my user ID and password is to be used only by me. Under no circumstances will I reveal or allow use of my password by another person.

I understand that inappropriate use of Data Broker information is a work rule violation and will result in disciplinary action up to and including dismissal, exercise of remedies for breach of contract, and/or termination of contract.

I agree to request Data Broker credit reports only when permissible purpose exists. I understand that "permissible purpose" means that the individual whose credit report I request must be:

- an applicant or recipient of TANF, Medicaid, or Food Stamps, or
- a household member who would be included in the TANF, Medicaid, or Food Stamp case except that he or she is disqualified or ineligible, or
- a member of the Medicaid budget group.

I have been informed that requesting a credit report without permissible purpose is a violation of federal law and may result in civil liability.

I understand that requesting a Data Broker credit report for purposes not associated with determining eligibility for Texas Works programs is a work rule violation and will result in a recommendation for dismissal, exercise of remedies for breach of contract, and/or termination of contract.

I understand and agree to follow the security procedures stated in this agreement.

______________________________	____________
Signature	Date

Computer Security Agreement

State On-Line Query System (SOLQ) - Wired Third Party Query System (WTPY)

I acknowledge that, as a receiving agency user, I have been assigned a personal user identification code (user ID) and password which I will use to activate the State On-Line Query System and/or Wired Third Party Query System, that allows access to information provided by the Social Security Administration. I understand that I will be held personally accountable for my actions and any activity performed under my password. Under no circumstances will I allow my user ID and confidential password to be used by any other individual, nor will I use one belonging to someone else. I will not enter any unauthorized data, make any unauthorized changes to data, or disclose any information without prior authorization. Intentionally violating a data security system or allowing unauthorized access by another party is a criminal offense under Chapter 33 of the Texas Penal Code. Depending on the circumstances and severity of the offense, such a crime may range from a Class B misdemeanor punishable by a fine of up to $2,000, 180 days in jail, or both to a first-degree felony punishable by a fine of up to $10,000 and not less than five years in jail.

I agree to abide by the Social Security Administration State On-Line Query System and/or Wired Third Party Query System information security operating procedures and standards. I also understand that if I violate any of these standards I may be subject to disciplinary action, exercise of remedies for breach of contract, contract termination, and/or prosecution under one or more applicable statutes, and that I may jeopardize the agreement between the Texas Department of Aging and Disability Services and the Social Security Administration.

Signature of User

Date

Computer Security Agreement

It should be emphasized that all individuals with access to DADS information resources have a responsibility for contributing to the security of equipment and information. Certain individuals may have primary responsibility, but all individuals have a role in protecting equipment and data. See *Automation and Telecommunications Handbook* (ATH), Section 3000.

All automated equipment operators have the responsibility to ask for names and purposes of visits from people who do not seem to be known by any staff in the area of the equipment. See ATH, Section 3000.

Whenever possible, screens of terminals should be placed so visitors or passersby cannot see confidential information on the screen. This may not be practical for single-user microcomputers. The back of a microcomputer should not be turned to the outside of the desk, as accidental powering off could occur. See ATH, Section 3000.

Do not use initials or something easily guessed for a password. The importance of keeping passwords confidential must be emphasized. See ATH, Section 3000.

Destroy all printouts and carbons from printouts according to procedures in Item B-11600, Records Destruction, in the *Administrative Management Handbook* (AMH). See AMH, Section B-11000.

Do not remove equipment from the premises without signing out the equipment with the data communications manager, office manager, or division administrator, or regional director for Texas Works or Long Term Care Services.

Any user sharing access is subject to appropriate termination of access. See ATH, Section 3000.

DADS policy regarding sharing use of state computer systems is included in the ATH, Section 3000. This policy covers usage of DADS hardware and software.

Data Integrity and Security

All use of agency owned or leased computer systems must be for officially authorized purposes only. The use of DADS computer systems for non-agency consulting work or unofficial purposes without the written approval of the commissioner is prohibited. The sale of DADS computer system time outside DADS requires the prior written approval of the commissioner.

All computer programs and data are for the sole use of DADS. All computer programs and data developed for DADS by consultants or vendors are the property of DADS and must be returned to DADS upon project completion or termination, unless a written release is granted by the commissioner.

The commissioner or designee is responsible for the proper authorization of computer utilization by the agency and the establishment of effective use.

MIS is responsible for the security and integrity of data in category 1 and 3 systems. For category 2 systems, the approving authority for a system or database is responsible for the integrity of data and its external and internal security.

Copies of any programs or data may only be released for DADS computer systems upon written authorization of the commissioner or designee.

Before the last day of work, all department property and equipment used in connection with computer systems must be returned.

Questions concerning the appropriateness of the release of a data file or computer program should be directed to the appropriate regional administrator, assistant commissioner, or supervisor.

Copyright laws have been made to protect the rights of both the users and the creators of documents and other original material. All users have the responsibility for avoiding copyright violations during use of automation technologies. This includes copying and altering licensed software and applies to systems software, application packages, documentation, and other material provided by vendors. System software must not be used on non-DADS equipment. See ATH, Section 3000.

Because client information is confidential, precautions must be taken to limit unauthorized access to client information. Requesters should submit requests for inquiries and disclosure of information. See AMH, Section A-8000.

By law, information in DADS files is confidential. Only authorized staff may change confidential information. It is unlawful to change, alter, or damage files without expressed permission. See Section 33.02, Texas Penal Code.

In addition to restricting unauthorized access to information on computer files, the operator must be aware of the limitations on releasing information on computer files. Additional restrictions are placed on requests from non-DADS users. If there is a question about the release of information, contact the supervisor.

All users are expected to not willfully or negligently damage, misuse, lose, or sell state property, department equipment, or materials for personal use or monetary gain. See *Human Resource Services Handbook*, Section 4700, Agency Rules and Requirements, and ATH, Sections 3500 and 4730.

Provider Agency Requirements

Except for purposes directly connected with the administration of the department's assistance programs, it is an offense for a person to solicit, disclose, receive, or make use of, or to authorize, knowingly permit, participate in, or acquiesce in the use of the names of, or any information concerning, persons applying for or receiving assistance if the information is directly or indirectly derived from the records, papers, files, or communications of the department or acquired by employees of the department in the performance of their official duties. See Texas Human Resources Code, Section 12.003.

The provider agency is responsible for notifying DADS of the termination of employment of any staff member who has signed a computer security agreement.

Computer Security Agreement

Users seeking access to IRS provided data, complete the top information portion of the Computer Security Agreement on page 1 of this form. It is optional if you want to complete the provider agency name section. Read the last four paragraphs on page 1, then sign and date the statements at the bottom of the page.

The four excerpts (exhibits 1-4 below) summarize the larger briefing material that is maintained with other policies and procedures within your unit.

Exhibit 1

Returns and return information shall be confidential.

During employment, as well as after a person terminates employment, laws preclude a person from disclosing tax return information.

Return information includes many pieces of information and is not limited to the taxpayer's name, source and amount of income, payments, deductions, and net worth.

This section also includes definitions of terms.

Exhibit 2

This section deals with safeguarding information. Ensure you apply rules approved by your management.

Follow the rules on destruction and storage of Federal Tax Information (FTI). (Only share information with an approved office or individual that is authorized to use FTI in the performance of duties.)

Exhibit 3

Exhibit three outlines the penalties for disclosing tax information.

Any violation is a felony and, if convicted, one can receive a fine up to $5,000 or be imprisoned for not more than five years.

It is also a felony to unlawfully receive FTI and disclose that information in a manner not approved by this title.

Exhibit 4

Exhibit four outlines the civil damages a person or an agency can incur for disclosing FTI.

No liability will occur if the disclosure is in good faith or at the request of the taxpayer.

Damages can be assessed at $1,000 per disclosure or the sum of the actual damages.

A plaintiff can file a complaint up to two years from time of discovery.